REMARKS

Applicants acknowledge that this application is currently under final rejection. Accordingly, a Request for Continued Examination has been submitted herewith, and further consideration of this application in view of the foregoing amendments and the following comments is respectfully requested.

Claims 1-17 have been rejected under 35 U.S.C. §102(b) as anticipated by Williams (Published U.S. Patent Application No. 2003/0005331). However, for the reasons set forth hereinafter, Applicants respectfully submit that all claims which remain of record in this application distinguish over the Williams application, whether considered by itself or in combination with other references.

The present invention is directed to a method for secure communication among computer user domains which are connected by a "connecting network". As is known to those skilled in the art, a "domain" is a network of computers that enables the computers which are connected thereto to communicate within the domain in a secure fashion. Computing systems frequently include multiple user domains or networks having different security clearance levels. In this case, it is necessary to protect data communicated between user domains of the same clearance level from unauthorized access -- via the connecting network -- by domains in the overall computing system which have a lower classification.

An important distinction between the present invention and the Williams publication is that the method according to the present invention is directed to the security of communications between networks, rather than between individual computers. In order to clarify this aspect of the invention, Claim 1 has been amended to recite that at least one of the user domains which is connected by the "connecting network" is itself "a network of a plurality of computers". Moreover, Claim 1 as amended further specifies that each of the user domains has a domain separator that is coupled in data communication with each computer that is connected to the network in question. The steps recited therein are then performed at a first user domain (network) for the purpose of sending information to a second user domain (network) via the connecting network. This aspect of the invention is illustrated, for example, in Figures 3-5 of the drawings, in which the connecting network (4 in Figure 3, 5 in Figure 4, and in 6 in Figure 5) is connected with multiple domains, each of which has a domain separator that is connected to each of the computers within the particular domain.

The Williams publication, on the other hand, discloses a system for controlling security among a plurality of computers, each of which has its own security device 18, as described, for example, at paragraph [0050], line 6 through paragraph [0052], line 4, as follows:

> The network 10 has security devices 18...installed between each host (work station 14 or server 16) in the local area network medium 20 to form a local area network (LAN) 5. The various LANs 5 are connected to an untrusted backboned net 30 by a router 22 .... The security device is self-contained circuit board that is directly integrated into the hardware of the host system .... Thus, the security cards 18 operate at the network layer (layer 3) of the protocol stack and provide encrypted, controlled communications from one host (IP address, TCP/UDP port) to another.

In other words, in Williams, each of the computers which is connected to one of the LANs itself contains a security device 18, so that all network security is provided at the level of the local device itself, an arrangement which is far more complex and costly than the present invention, in which each domain contains a domain separator that is coupled to all computers contained within that network, such that the domain separator for a particular network provides security functionality for all computers contained in that network. In Williams, each security device checks the security level of the data to be transmitted over the network by the computer in which it is integrated. A network security computer (NSC) controls and administers the operation of the security devices of the respective computers.

Unlike Williams, the present invention, as defined in Claim 1, needs only to operate at the network level, eliminating the need for a security device at each

computer. Network traffic that leaves the network is tagged and turned into a datagram appended with a check sum, etc. and sent to another secure network. If the receiving network is appropriate and cleared, it will be able to verify the received datagram and transmit the data onto the receiving secure network. This arrangement has the further advantage that, within a secure network, data can pass freely with no delay or need for expensive security devices. Rather, the data is secured only when it is transmitted over an unsecure network.

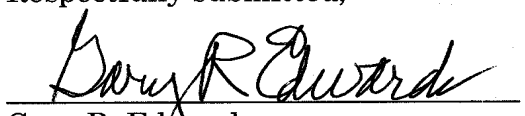
For the reasons set forth above, Applicants respectfully submit that Claim 1, and therefore all claims of record, distinguish over the Williams publication, and are allowable.

In light of the foregoing remarks, this application should be in consideration for allowance, and early passage of this case to issue is respectfully requested. If there are any questions regarding this amendment or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and

please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket #038665.56061US).

Respectfully submitted,



Gary R. Edwards
Registration No. 31,824

CROWELL & MORING LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
GRE:kms
4274788_1